(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 437 616 A1**

(12) **EUROPEAN PATENT APPLICATION published in accordance with Art. 158(3) EPC**

(21) Application number: **90909364.3**

(22) Date of filing: **15.06.90**

(86) International application number: **PCT/JP90/00785**

(87) International publication number: **WO 91/01892 (21.02.91 91/05)**

(51) Int. Cl.5: **B42D 15/10**, G06K 17/00, G06K 19/00, G07F 7/08

(30) Priority: **26.07.89 JP 191327/89**

(43) Date of publication of application: **24.07.91 Bulletin 91/30**

(84) Designated Contracting States: **DE FR GB**

(71) Applicant: **NTT DATA COMMUNICATIONS SYSTEMS CORPORATION**
26-5 Toranomon 1-chome, Minato-ku
Tokyo 105(JP)

(72) Inventor: **HAMADA, H. NTT Data Comm. Systems Corp.**
26-5, Toranomon 1-chome Minato-ku
Tokyo 105(JP)

Inventor: **HIRANO, K. NTT Data Comm.Systems Corp.**
26-5, Toranomon 1-chome Minato-ku
Tokyo 105(JP)

Inventor: **LEE, Y., S. NTT Data Comm. Systems Corp.**
26-5, Toranomon 1-chome Minato-ku
Tokyo 105(JP)

(74) Representative: **Schmidt-Evers, Jürgen, Dipl.-Ing. et al**
Patentanwälte Mitscherlich, Gunschmann Dr. Körber, Schmidt-Evers, Melzer, Dr. Schulz
Steinsdorfstrasse 10
W-8000 München 22(DE)

(54) **IC CARD SYSTEM HAVING FUNCTION OF CONFIRMING DESTROYED DATA.**

(57) An IC card contains an IC chip including a cipher processing circuit in addition to an ordinary data record processing circuit, and further possesses a magnetic or optical data recording portion provided on the card. In the magnetic or optical data recording portion on the IC card are recorded data at the time of initialization and at the final transaction in a predetermined enciphered form by the cooperation of an initializing terminal unit, a transaction terminal unit and the IC chip in the IC card. In case the data recorded in the IC chip in the IC card are destroyed, a confirmation terminal unit decodes the data recorded on the magnetic or optical data recording portion to make sure their validity. When it is confirmed that the data decoded by the confirmation terminal unit are valid, the initialization terminal unit restores them in a new IC card.

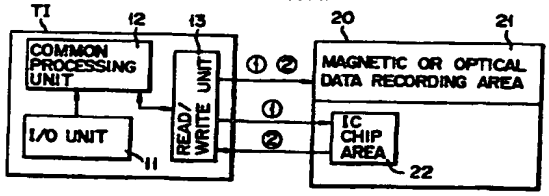

FIG. 1

EP 0 437 616 A1

[TECHNICAL FIELD]

The present invention relates to an IC card system and, in particular, an IC card system of such a type that, even if, upon the use of an IC card as a "prepaid" card for instance, data is found to be destroyed owing to a damaged IC chip, etc., data items, such as a "prepaid" balance, recorded in the IC card can be identified by the IC card and the terminal in a self-solving way without using any large-scaled on-line system and restored with added safety.

[Background Art]

A prepaid card, such as a conventional prepaid telephone card, is not safe from the standpoint of security, such as the protection of secret data and prevention of tampering. In the conventional prepaid card system, when data items in the prepaid card are maliciously or inadvertently destroyed by a card owner or any third party, there is no safe countermeasure for restoring data on a "prepaid" balance.

An IC card equipped with an IC version of a data storing/processing circuit is outstandingly superior to other cards form the standpoint of security, such as the protection of secret data and prevention of the tampering of data.

There is a relatively high possibility that, because such an IC chip is embedded in a plastics card, data items in the card will be destroyed, not to mention a damage to the IC itself. Further, in the event of the data items being destroyed in the card, it is not possible to identify data, such as a "prepaid" balance. Even if any dispute arises between a card owner and a card issuing person in connection with the "prepaid" balance, there has been no effective solution to such a problem.

There is, therefore, a growing demand for identifying and restoring data items in the IC card system as set out above. An effective measure, therefore, is necessary to readily identify damaged data without using any large-scaled on-line system and to prevent any possible misuse upon the reissuing of an IC card.

[Disclosure of Invention]

It is an object of the present invention to provide an improved IC card system in which final transaction data items, once disturbed by encryption, are recorded in a magnetic or optical data recording unit whereby, when data items in the IC card are destroyed, the recorded data items are read out of the data recording unit to enable the read-out data items to be readily identified for their truth.

Another object of the present invention is to provide an IC card system which, when data items read out of a magnetic or optical data recording unit is proved true, restores the true data items in a new IC card.

According to the present invention, there is provided on IC card system for enabling data which is stored in an IC card equipped with an IC chip area and a magnetic or optical data recording area at its predetermined area to be authenticated in cooperation with a predetermined terminal, the system characterized by comprising:

a first unit for enabling data which is associated with a final transaction by the IC card to be subjected to a predetermined processing, including an encryption processing, by a predetermined data process made between an encrypting area stored in an IC area of the IC card and a read/write unit in a terminal for identification and between the read/write unit and a common processing units;

a second unit for enabling data which is subjected by the first means to the processing to be transferred to the magnetic or optical data recording area via the read/write unit on the terminal and to be recorded there; and

a third unit for enabling the processed data associated with the final transaction which is recorded on the magnetic or optical data recording area to be subjected to a predetermined re-processing, including a decryption processing at the read/write unit and common processing unit, when the data in the IC area of the IC card is destroyed, and for authenticating truth of the data.

According to another aspect of the present invention, an IC card system includes a fourth unit which, when the truth of the data re-processed by the third unit is authenticated, transfers that data from the terminal for identification to the terminal for initialization and restores it into a new card.

In summary, the present IC card system comprises:

a first unit for performing a predetermined data processing, including an encryption processing, relative to an initializing or transaction terminal in cooperation with an IC card and an code preparation unit in the IC card;

a second unit for recording final transaction data in a magnetic or optical data recording area of the IC card after it has been disturbed by a predetermined code; and

a third unit for decrypting the data of the recording unit by the identifying terminal, when it is needed for restoration, so that it is identified for truth. The present IC card system further com-

prises a fourth unit which, when the data is proved true, enables data on a "prepaid" balance, etc., to be restored by the initializing terminal for re-issuing of a new IC card.

In the IC card system as set out below, when an IC chip of the IC card is inaccessible due to its damage, etc., the card owner requests the card issuing person to restore data on, for example, a "prepaid" balance so that it is re-issued.

The card issuing person re-processes final transaction data of the magnetic or optical data recording area through decryption with the use of an identifying terminal, for example, a card owner's built-in code function F and code key and prepares an identification code and compares it with an identification code which is read, as a to-be-re-processed data, out of the magnetic or optical data recording area. If there is a coincidence between the two, the card issuing person authenticates it as being true, restores the final transaction data and issues a novel IC card.

[Brief Description of the Drawings]

Figs. 1 to 3 show an IC card system according to one embodiment of the present invention, Fig. 1 showing a state of a connection between an initializing terminal and an IC card as well as a data transfer between them and its control, Fig. 2 showing a state of a connection between a transaction terminal and an IC card as well as a data transfer between them and its control, and Fig. 3 showing a state of a connection between the IC card and an identifying terminal for identifying data of a magnetic or optical data recording area when data once stored in the IC card, if damaged, is restored, as well as a data transfer between the IC card and the terminal and its control.

[Best Mode of Carrying Out the Invention]

An IC card system according to one embodiment of the present invention will be explained below with reference to the accompanying drawings.

Fig. 1 shows a state of a connection between an initializing terminal unit T1 and an IC card 20 and a data transfer between the two and its control which constitute one aspect of a restoration device of the present invention.

An initializing terminal unit T1 which is placed under complete control of an IC card issuer as his or her agent includes an input/output unit 11, common treating units 12 and read/write unit 13. The IC card 20 is initialized by the terminal T1 and handed over to a specific person who becomes a card owner.

The IC card 20 to be used by the card owner includes a magnetic/optical data recording area 21 and IC chip area 22.

The IC chip area 22 includes, in addition to an ordinary data storing/processing unit, a circuit (a code preparing unit) for processing a code function (F), both of which are absolutely inaccessible from an outside. A code key KUC which is unique to the IC card 20 is accessible by only a specific terminal, etc., which is owned or designated by a card issuer, and is initially stored in a chip area 22 of the IC card.

Those items of issuing data (that is, issuing data TD (1)) as input from the input/output unit 11 in the terminal unit T1 or automatically generated from the processing unit 12 are stored as initial history data into the IC ship area 22 of the IC card 20 from the read/write unit 13 in the initializing terminal unit T1, the items of data containing the data of issuing, place-of-issuing (initializing terminal ID) code, amount of money received upon issuance, a "prepaid" balance upon issuance, etc.

A symbol (1) in the issuing data TD (1) represents the transfer of data on the drawing sheet. The same thing can be applied to those items of data and code as will be set forth below.

The data TD (1) and authentication code (hereinafter referred to as [identification code TC (2)] generated based on the data TD (1) are registered in the magnetic/optical data storing area 21 of the IC card 20.

The identification code TC (2) is a multi-digit code uniquely determined by the issuing data TD (1), that is, a result of an arithmetic operation obtained in accordance with a function F using the code key KUC and transaction data TD (1), the function F being incorporated into the chip area 22 in the IC card 20. The code TC (2) is taken into the IC card via the read/write unit 13 in the terminal unit T1.

The terminal unit T1 encrypts the identification code TC (2) together with the data TD (1) and delivers it via the read/write unit 13 to the magnetic or optical data recording unit 21 where it is stored.

A relation among the code function F, data TD, identification code TC and code key KUC is represented by:

$$TC = F(TD, KUC)$$

Fig. 2 shows a data transfer, that is, goods or services transferred, by a prepaid action, with the use of a user IC card UC which has been given to the card owner after initialization.

Fig. 2 shows the case where a card owner insert or loads the user IC card UC into a transaction terminal unit TT as installed at a shop and street corner.

Those items of transaction data (hereinafter

referred to as transaction data TD (1) for the sake of convenience) entered from an output section (an input/output unit 11A) of the transaction terminal TT or automatically generated from a common control unit 12A are added to a history at a time of card issuance, or updated via a read/write unit 13A, the transaction data containing a transaction data, site-of-transaction (terminal) code, amount of transaction, "prepaid" balance, prepayment and so on and being the same format as that of the aforementioned issuing data TD (1).

Transaction data TD (1) involved in a final transaction as well as an authentication code (hereinafter referred to as an identification code TC (2) for the sake of convenience) generated in the same format as that of the identification code TC (2) is encrypted via the read/write unit 13A and written into a magnetic/optical data storing area 21A in the user IC card UC.

Although a step of charging or receiving a price or a payment for goods and services, by a goods/services provider or an agent, as a result of a transaction is omitted for brevity's sake, it is done in the process substantially the same as set forth above.

Let it be assumed that data in the chip area 22A in the user IC card UC cannot be read out due to a breakage, etc., of the IC chip area 22A and that a transaction fails to continue owing to a "prepaid" balance being placed in an inaccessible state.

In this case, the owner of the user IC card presents a defective IC card UC to the card issuing person or his or her agent, claiming that a "prepaid" balance should be guaranteed. The card issuing person or his or her agent handles a restoring terminal TA as shown in Fig. 3 in accordance with the claim of the card owner and restores and identifies that "prepaid" balance. The card issuing person or his or her agent takes a proper step, such as the reissuing of an IC card to guarantee the "prepaid" balance.

That is, on the side of the card issuing person or his or her agent, a code key kUC of the user IC card UC is arithmetically operated on by the terminal TA in accordance with a secret key KAC and the same function F as a code function built in the user IC card UC of the card owner as well as a card recognition data recorded in magnetic or optical data recording unit 21B inscribed in the IC card, noting that the key KAC and function F can be stored in an authentication-only IC card so as to further enhance a security level. An identification code TC (3) is generated, in the same way as set out above, form the code key KUC thus obtained and transaction data TD (1) in those items of data read out of the magnetic or optical data recording area 21B. This identification code (3) is compared with an identification code TC (2) in those data items which are read out of the magnetic or optical data recording area 21B.

If a coincidence occurs as a result of comparison, the transaction data TD1 in the data items read out of the magnetic or optical data recording area 21A can be regarded as being not maliciously altered by something.

The card issuing person or his or her agent performs an issuing operation of a new IC card 20 (UC), in accordance with the sequence as set out in connection with Fig. 1, with the use of a "prepaid" balance on a final transaction in the read-out transaction data TD (1).

Although the present embodiment has been explained in connection with the present invention, when the transaction terminal TT delivers transaction data TD (1) and identification code TC (2) to the magnetic or optical data recording area, TD (1) and TC (2) are encrypted as a whole for enhanced security to place an encrypted one generally under an inaccessible state and encryption is done prior to the process of restoring and identifying data, such as a "prepaid" balance, regarding a final transaction by the terminal TA. This modification constitutes an extension and hence another application which is covered by the present invention.

The IC card system of the present invention is operated as set out above. That is, the final transaction data of the IC card, once disturbed by the code, is registered in the magnetic or optical data recording area. It is, therefore, difficult for any malicious person to read out the final transaction data. Even if the data is tampered with, identification can be made, upon request by the IC card owner, on the card issuing person's side whether or not the data in the magnetic or optical recording area is tampered with. Since data, such as a "prepaid" balance cannot be restored in a new IC card unless the card owner confirms the truth of the data, it is possible to prevent any misuse of the card upon re-issuing of it.

Since the present IC card system has the features as set out above, if the card owner asks the card issuing person to replace a damaged card by a new one, the person can readily confirm the truth of final transaction data in the IC card without using any large-scaled on-line system and re-issue a new IC card with a restored true "paid" balance, etc., registered therein, preventing any trouble from arising between the card issuing person and the card owner. The present IC card system ensures high security and hence very high satefty.

[Industrial Applicability]

The present invention can be applied to an IC card system, in general, performing, for example,

an individual authentication, data management and credit transaction.

Claims

1. An IC card system for enabling data which is stored in an IC card equipped with an IC chip area and a magnetic or optical data recording area at its predetermined area to be authenticated in cooperation with a predetermined terminal, the system characterized by comprising:

   first means for enabling data which is contained in connection with a final transaction by the IC card to be subjected to a predetermined processing, including an encryption processing, by a predetermined data process made between an encrypting area stored in an IC area of the IC card and a read/write unit in a terminal for identification and between the read/write unit and a common processing unit;

   second means for enabling data which is subjected by the first means to the processing to be transferred to the magnetic or optical data recording area via the read/write unit on the terminal and to be recorded there; and

   third means for enabling the processed data associated with the final transaction which is recorded on the magnetic or optical data recording area to be subjected to a predetermined re-processing, including a decryption processing at the read/write unit and common processing unit, when the data in the IC area of the IC card is destroyed, and for authenticating truth of the data.

2. The system according to claim 1, characterized by further comprising fourth means which, when the truth of the data re-processed by said third means is authenticated, transfers that data from said terminal for identification to said terminal for initialization and restores it into a new IC card.

3. The system according to claim 1, characterized in that said authenticated data contains data on a prepaid balance.

Amended claims

1. (Amended) An IC card system for enabling data which is stored in an IC card equipped with an IC chip area and a magnetic or optical data recording area at its predetermined area to be authenticated in cooperation with a predetermined terminal, the system characterized by comprising:

   first means for enabling data which is contain in connection with a final transaction by the IC card to be subjected to a processing with a transaction authentication code generated in accordance with a code function and authentication individual key specific for the IC card, the processing being done through a predetermined data processing made between a common processing unit and the read/write unit in a terminal for initialization or for transaction.

   second means for enabling data which is subjected by the first means to the processing to be transferred to the magnetic or optical data recording area via the read/write unit on the terminal and to be recorded there; and

   third means for enabling the processed data associated with the final transaction which is recorded on the magnetic or optical data recording area to be checked for truthness with the use of a code or decording function of the read/write unit and common processing unit, when the data in the IC area of the IC card is destroyed.

2. (Amended) The system according to claim 1, characterized by further comprising fourth means which, when the truth of the data checked by said third means is authenticated, transfers that data from said terminal for identification to said terminal for initialization and restores it into a new IC card.

3. The system according to claim 1, characterized in that said authenticated data contains data on a prepaid balance.

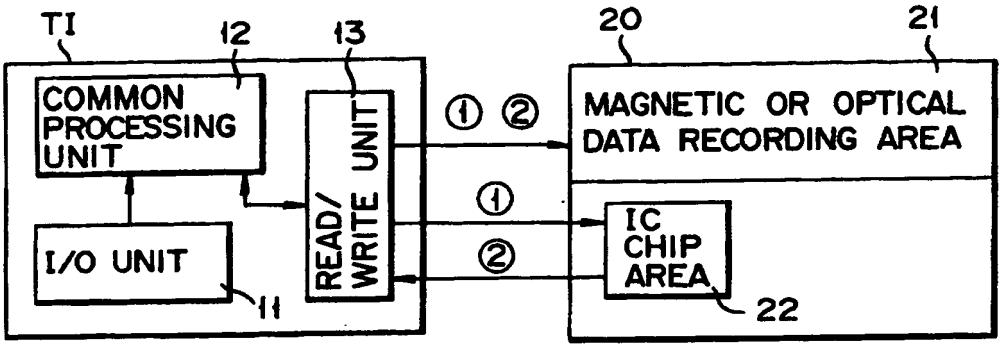

FIG. 1

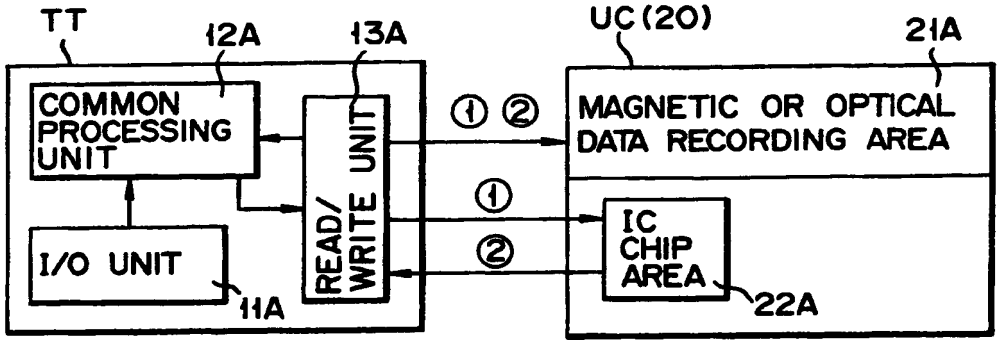

FIG. 2

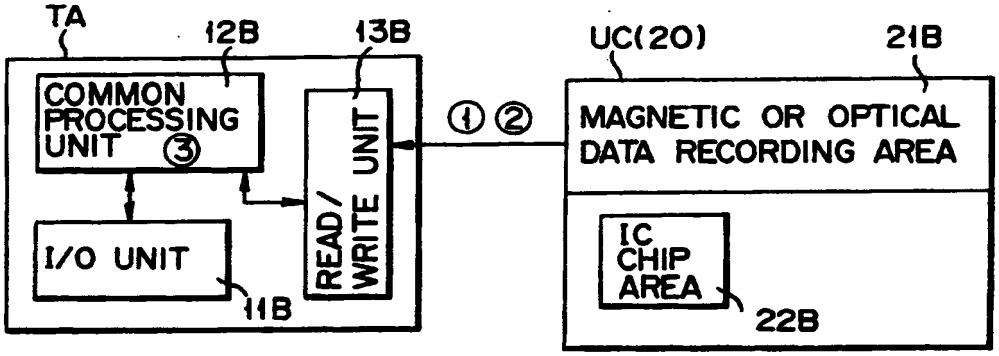

FIG. 3

INTERNATIONAL SEARCH REPORT

International Application No PCT/JP90/00785

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [6]

According to International Patent Classification (IPC) or to both National Classification and IPC

Int. Cl[5] B42D15/10, G06K17/00, 19/00, G07F7/08

II. FIELDS SEARCHED

Minimum Documentation Searched [7]

Classification System	Classification Symbols
IPC	G06K17/00, 19/00

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched [8]

Jitsuyo Shinan Koho	1975 - 1989
Kokai Jitsuyo Shinan Koho	1975 - 1989

III. DOCUMENTS CONSIDERED TO BE RELEVANT [9]

Category [10]	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No. [13]
Y	JP, A, 58-94132 (Dai Nippon Printing Co., Ltd.), 4 June 1983 (04. 06. 83), (Family: none)	1 - 3
Y	JP, A, 60-84686 (Toshiba Corp.), 14 May 1985 (14. 05. 85) & US, A, 4,672,182 & EP, B1, 138,219	1 - 3
Y	JP, A, 62-219192 (Fujitsu, Ltd.), 26 September 1987 (26. 09. 87), (Family: none)	1 - 3
Y	JP, A, 63-74696 (Hitachi, Ltd.), 5 April 1988 (05. 04. 88), (Family: none)	1 - 3
Y	JP, A, 63-288383 (Nippon Electric Co., Ltd.), 25 November 1988 (25. 11. 88), (Family: none)	1 - 3

* Special categories of cited documents: [10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
September 5, 1990 (05. 09. 90)	September 17, 1990 (17. 09. 90)

International Searching Authority	Signature of Authorized Officer
Japanese Patent Office	

FURTHER INFORMATION CONTINUED FROM THE SECOND SHEET

Y	JP, A, 64-81087 (Hitachi Maxell, Ltd.), 27 March 1989 (27. 03. 89), (Family: none)	1 - 3
Y	JP, A, 61-217886 (Computer Service K.K.), 27 September 1986 (27. 09. 86), (Family: none)	3
A	JP, A, 63-61393 (Dai-ichi Denshi Kogyo K.K.), 17 March 1988 (17. 03. 88), (Family: none)	1 - 3

V. ☐ OBSERVATIONS WHERE CERTAIN CLAIMS WERE FOUND UNSEARCHABLE [1]

This international search report has not been established in respect of certain claims under Article 17(2) (a) for the following reasons:

1. ☐ Claim numbers . because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claim numbers , because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claim numbers , because they are dependent claims and are not drafted in accordance with the second and third sentences of PCT Rule 6.4(a).

VI. ☐ OBSERVATIONS WHERE UNITY OF INVENTION IS LACKING [2]

This International Searching Authority found multiple inventions in this international application as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims of the international application.

2. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims of the international application for which fees were paid, specifically claims:

3. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claim numbers:

4. ☐ As all searchable claims could be searched without effort justifying an additional fee, the International Searching Authority did not invite payment of any additional fee.

Remark on Protest

☐ The additional search fees were accompanied by applicant's protest.

☐ No protest accompanied the payment of additional search fees.